

token to authenticate the first computer;

authenticating the first computer using the authentication token in the service request message;

ascertaining a password from the authentication token from the first computer;

determining whether the password from the first computer matches a stored password in the second computer;

determining validity of the password at the second computer at the second computer if the password matches the stored password, wherein the determining the validity of the password comprises

ascertaining a current time at which the service request message is received,

determining a first time statement indicating a time at which the password is formed, and

determining a second time statement indicating a period of time for which the password is valid, wherein the password is valid if the current time is less or equal to a summation of the first time statement and the second time statement;

providing the service request to the first computer if the password is valid;

transmitting to the first computer an updated message requesting that the password be updated if the password is invalid;

receiving at the second computer a password message transmitted by the first computer, wherein the password message comprises an integrity statement to check the integrity of the password message from the first computer;

checking the integrity of the password message;

ascertaining the updated password; and

storing in the second computer the updated password and providing the service to the first computer.

---

#### **REMARKS**

This Preliminary Amendment is submitted to improve the form of the specification as originally-filed. It is respectfully requested that this Preliminary Amendment be entered in the above-referenced application.

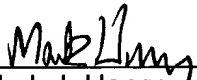
In accordance with the foregoing, claims 16 and 27 have been amended and claims 36-63 have been added. Claims 13-63 are pending and are under consideration.

If there are any questions regarding these matters, such questions can be addressed by telephone to the undersigned. Otherwise, an early action on the merits is respectfully solicited. If any further fees are required in connection with the filing of this Preliminary Amendment, please charge same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

By:

  
\_\_\_\_\_  
Mark J. Henry  
Registration No. 36,162

700 Eleventh Street, N.W.  
Suite 500  
Washington, D.C. 20001  
(202) 434-1500  
Date: June 27, 2001

**VERSION WITH MARKINGS TO SHOW CHANGES MADE****IN THE CLAIMS:**

Please AMEND the following claims:

16. (ONCE AMENDED) The method as claimed in claim 15, wherein the password message contains the updated password in an encrypted form, [the] a key for encrypting the updated password being formed on the basis of the password.

27. (ONCE AMENDED) At least one computer readable medium storing at least one program for controlling [at least one] a first computer and a second computer to perform a method comprising:

receiving at the second computer a service request message transmitted by the first computer over a communication link existing between the first computer and the second computer, the service request message containing the password, and being used to request provision of a service;

checking, at the second computer, whether the password contained in the service request message is valid for the first computer;

if the password is valid, providing the service;

if the password is invalid, transmitting from the second computer to the first computer an update message to request that the password be updated; and

forming an updated password.

Please ADD following new claims.

36. (NEW) A method for updating a password, comprising:

receiving a service request message, the service request message comprising the password and being used to request a service;

checking whether the password contained in the service request message is valid;

providing the service if the password is valid;

transmitting an update message to request that the password be updated if the password is invalid; and

forming an updated password.

37. (NEW) The method as claimed in claim 36, wherein after the updated password is

formed, the service request message comprises the updated password and further comprising checking whether the updated password is valid.

38. (NEW) The method as claimed in claim 36, wherein the forming the updated password comprises:

receiving a password message containing the updated password,  
using the password to ascertain the updated password from the password message,  
and  
storing the updated password.

39. (NEW) The method as claimed in claim 38, wherein the password message contains the updated password in an encrypted form, a key for encrypting the updated password being formed based on the password.

40. (NEW) The method as claimed in claim 38, further comprising transmitting an acknowledgment message acknowledging the use of the updated password within the context of the communication link.

41. (NEW) The method as claimed in claim 36, wherein the checking whether the password contained in the service request message is valid is performed using a monitor database indicating whether an update message has been previously transmitted.

42. (NEW) The method as claimed in claim 36, further comprising  
checking the received service request message for its integrity, wherein the password is checked only if the integrity of the service request message is ensured and, if the integrity of the service request message is not ensured, the requested service is refused, wherein the service request message comprises a statement relating to integrity protection.

43. (NEW) A method for updating a password, comprising:  
receiving a service request message requesting a service and comprising an authentication token;  
ascertaining a password from the authentication token;  
determining whether the password matches a stored password;

determining validity of the password if the password matches a stored password;  
providing the service if the password is valid;  
transmitting an update message requesting that the password be updated if the password is invalid;  
receiving a password message comprising an updated password;  
checking the integrity of the password message;  
ascertaining the updated password using the password; and  
storing the updated password and providing the service.

44. (NEW) The method as recited in claim 43, wherein the validity of the password is determined by  
ascertaining a current time at which the service request message is received,  
determining a first time statement indicating a time at which the password is formed, and  
determining a second time statement indicating a period of time for which the password is valid, wherein the password is valid if the current time is less or equal to a summation of the first time statement and the second time statement.

45. (NEW) A method for updating a password of a computer, comprising:  
receiving a service request message requesting a service and comprising an authentication token;  
authenticating the computer using the authentication token in the service request message;  
ascertaining a password from the authentication token;  
determining whether the password matches a stored password;  
determining validity of the password if the password matches a stored password;  
providing the service if the password is valid;  
transmitting to the computer an update message requesting that the password be updated if the password is invalid;  
receiving a password message from the computer comprising an updated password, where the updated password can be ascertained only by using the password;  
checking the integrity of the password message;  
ascertaining the updated password using the password; and  
storing the updated password and providing the service.

46. (NEW) The method as recited in claim 45, wherein the validity of the password is determined by

- ascertaining a current time at which the service request message is received,
- determining a first time statement indicating a time at which the password is formed, and
- determining a second time statement indicating a period of time for which the password is valid, wherein the password is valid if the current time is less or equal to a summation of the first time statement and the second time statement.

47. (NEW) The method as recited in claim 45, wherein the password message comprises an integrity statement used to check the integrity of the password message.

48. (NEW) The method as recited in claim 45, wherein the authentication token permits the password to be presented in an encrypted form or in a one-way hash function form.

49. (NEW) A method for updating a password between a first computer and a second computer, comprising:

- entering via the first computer a criteria for a database query;
- receiving at the second computer a service request message based on the database query, the service request message requesting a service and comprising an authentication token to authenticate the first computer;
- authenticating the first computer using the authentication token in the service request message;
- ascertaining a password from the authentication token from the first computer;
- determining whether the password from the first computer matches a stored password in the second computer;
- determining validity of the password at the second computer at the second computer if the password matches the stored password, wherein the determining the validity of the password comprises
  - ascertaining a current time at which the service request message is received,
  - determining a first time statement indicating a time at which the password is formed, and
  - determining a second time statement indicating a period of time for which the

password is valid, wherein the password is valid if the current time is less or equal to a summation of the first time statement and the second time statement;

providing the service request to the first computer if the password is valid;

transmitting to the first computer an updated message requesting that the password be updated if the password is invalid;

receiving at the second computer a password message transmitted by the first computer, wherein the password message comprises an integrity statement to check the integrity of the password message from the first computer;

checking the integrity of the password message;

ascertaining the updated password; and

storing in the second computer the updated password and providing the service to the first computer.

50. (NEW) A computer readable storage medium controlling a computer and comprising a process of

receiving a service request message, the service request message comprising the password and being used to request a service;

checking whether the password contained in the service request message is valid;

providing the service if the password is valid;

transmitting an update message to request that the password be updated if the password is invalid; and

forming an updated password.

51. (NEW) The computer readable storage medium as claimed in claim 50, wherein after the updated password is formed, the service request message comprises the updated password and further comprising checking whether the updated password is valid.

52. (NEW) The computer readable storage medium as claimed in claim 50, wherein the forming the updated password comprises:

receiving a password message containing the updated password,

using the password to ascertain the updated password from the password message,

and

storing the updated password.

53. (NEW) The computer readable storage medium as claimed in claim 52, wherein the password message contains the updated password in an encrypted form, a key for encrypting the updated password being formed based on the password.

54. (NEW) The computer readable storage medium as claimed in claim 52, further comprising transmitting an acknowledgment message acknowledging the use of the updated password within the context of the communication link.

55. (NEW) The computer readable storage medium as claimed in claim 50, wherein the checking whether the password contained in the service request message is valid is performed using a monitor database indicating whether an update message has been previously transmitted.

56. (NEW) The computer readable storage medium as claimed in claim 50, further comprising

checking the received service request message for its integrity, wherein the password is checked only if the integrity of the service request message is ensured and, if the integrity of the service request message is not ensured, the requested service is refused, wherein the service request message comprises a statement relating to integrity protection.

57. (NEW) A computer readable storage medium controlling a computer and comprising a process of

receiving a service request message requesting a service and comprising an authentication token;

ascertaining a password from the authentication token;

determining whether the password matches a stored password;

determining validity of the password if the password matches a stored password;

providing the service if the password is valid;

transmitting an update message requesting that the password be updated if the password is invalid;

receiving a password message comprising an updated password;

checking the integrity of the password message;



ascertaining the updated password using the password; and  
storing the updated password and providing the service.

58. (NEW) The computer readable storage medium as recited in claim 57, wherein the validity of the password is determined by  
ascertaining a current time at which the service request message is received,  
determining a first time statement indicating a time at which the password is formed, and  
determining a second time statement indicating a period of time for which the password is valid, wherein the password is valid if the current time is less or equal to a summation of the first time statement and the second time statement.

59. (NEW) A computer readable storage medium controlling a computer and comprising a process of:

receiving a service request message requesting a service and comprising an authentication token;  
authenticating the computer using the authentication token in the service request message;  
ascertaining a password from the authentication token;  
determining whether the password matches a stored password;  
determining validity of the password if the password matches a stored password;  
providing the service if the password is valid;  
transmitting to the computer an update message requesting that the password be updated if the password is invalid;  
receiving a password message from the computer comprising an updated password, where the updated password can be ascertained only by using the password;  
checking the integrity of the password message;  
ascertaining the updated password using the password; and  
storing the updated password and providing the service.

60. (NEW) The computer readable storage medium as recited in claim 59, wherein the validity of the password is determined by  
ascertaining a current time at which the service request message is received,  
determining a first time statement indicating a time at which the password is formed, and

determining a second time statement indicating a period of time for which the password is valid, wherein the password is valid if the current time is less or equal to a summation of the first time statement and the second time statement.

61. (NEW) The computer readable storage medium as recited in claim 59, wherein the password message comprises an integrity statement used to check the integrity of the password message.

62. (NEW) The computer readable storage medium as recited in claim 59, wherein the authentication token permits the password to be presented in an encrypted form or in a one-way hash function form.

63. (NEW) A computer readable storage medium controlling a first computer a second computer and comprising a process of

- entering via the first computer a criteria for a database query;

- receiving at the second computer a service request message based on the database query, the service request message requesting a service and comprising an authentication token to authenticate the first computer;

- authenticating the first computer using the authentication token in the service request message;

- ascertaining a password from the authentication token from the first computer;

- determining whether the password from the first computer matches a stored password in the second computer;

- determining validity of the password at the second computer at the second computer if the password matches the stored password, wherein the determining the validity of the password comprises

  - ascertaining a current time at which the service request message is received,

  - determining a first time statement indicating a time at which the password is formed, and

  - determining a second time statement indicating a period of time for which the password is valid, wherein the password is valid if the current time is less or equal to a summation of the first time statement and the second time statement;

  - providing the service request to the first computer if the password is valid;

transmitting to the first computer an updated message requesting that the password be updated if the password is invalid;

receiving at the second computer a password message transmitted by the first computer, wherein the password message comprises an integrity statement to check the integrity of the password message from the first computer;

checking the integrity of the password message;

ascertaining the updated password; and

storing in the second computer the updated password and providing the service to the first computer.

password is invalid; and

forming an updated password.